Remarks/Arguments

This application was filed on October 12, 2001.

A first Office Action rejecting all 20 pending claims was mailed on or about January 26, 2005. An amendment and response to the January 26, 2005 office action was filed on or about April 26, 2005. The April 26, 2005 Response included an amendment to claim 1.

A final office action was mailed on June 28, 2005 rejecting all claims on the same grounds as the January 26, 2005 office action.

Claims 1-20 are pending and stand rejected on varying grounds under §102(e).

No claims have been amended, canceled or added.

In view of the comments below, Applicant respectfully requests that the Examiner reconsider the present application including claims 1-20 and withdraw the rejection of these claims.

a) Claims 1-20 stand rejected under 35 U.S.C. 102(e) as being clearly anticipated by Joyce (US Patent No. 6,519,703).

Claims 1 and 11 are in independent form with claims 2-10 dependent on claim 1 and claims 12-20 dependent on claim 11. The present invention concerns node security in a router of a packet network. Claim 1 defines a method for providing node security in the router of the packet network and claim 11 defines in varying scope a corresponding router for providing node

security in a packet network. Generally the invention includes analyzing a data packet and determining in the router whether the data packet may be harmful to a destination device and if so, transmission of the packet is interrupted and a second router is communicated with to cause the second router to interrupt transmission of a next or future data packet all as claimed. If no problems are detected the data packet is transmitted.

The Examiner maintains that Joyce teaches and describes a method and router for providing node security in a router of a packet network referring to Fig. 1, 2; Summary and Column 2, line 16 - Column 5, line 17.

Applicant concedes that the firewall arrangement of Joyce deals with security in a packet network and that the firewall arrangement may be construed as a router. Applicant however notes that Applicant is not claiming all methods and routers for providing node security, rather only those as specifically claimed.

Joyce discusses a firewall arrangement (FIG. 1 and FIG. 2) that may operate on a Sun MicroSystem computer or the like (col. 5, line 34 et. sequence), i.e., operates on one computer and thus is at most one router. This firewall (Heuristic firewall 10A or 10B) receives data packets 22 from the Internet, performs one or more "levels" of analysis on these packets (16, 18, 20 and 12, 14 among others), and shunts packets (i.e., interrupts transmission) that appear to have problems (low confidence) to a shunt 30 (log or the like), and forwards packets that have high confidence to a network 30 (FIG. 1, FIG. 2, and corresponding descriptions).

Issue I: Whether Joyce anticipates claim 1 or claim 11, i.e., whether Joyce shows or suggests all features of claim 1.

Applicant respectfully submits that Joyce does not show or suggest, in the context as recited by claim 1 (analogously by claim 11) "interrupting transmission of the data packet in response to determining that the data packet is potentially harmful to the destination device, the interrupting further comprising the step of communicating with a second router to cause the second router to interrupt transmission of a future data packet;".

The Examiner maintains that Joyce teaches the interrupting feature, this feature including the communication with a second router to cause the second router to interrupt a future data packet at (Column 2 line 30 - Column 3 line 5). Applicant concedes that Joyce shows a router and method that interrupts transmission of potentially harmful data packets. However, Applicant is unable to construe in good faith the discussions of Joyce to show the Joyce router as communicating with another router as claimed and respectfully submits that one of ordinary skill in the field would not interpret the Joyce firewall as showing more that one router. This is supported by a quick web search for Router definition and scanning the results.

Joyce discusses poor-confidence packets being shunted out of the firewall 10A and these may be subjected to further analysis or a connection may be established with a network simulator (not shown) to encourage a "cracker" to continue ...; however shunting for further analysis is not communicating with a second router to interrupt future packets as claimed. Marginal confidence

packets are released to a more complex firewall rule base 14 for processing (see col. 2, lines 51-65); however a rules base is not a second router and nothing is said about future packets. Unacceptable packets may be written to an exceptions log for later review or data can be forwarded for analysis (col. 3, lines 1-3); however this is not communicating with a second router pursuant to the claimed ends. High confidence or good confidence packets are released from a first buffer 24 to a traditional firewall rule base 12 (col. 2 lines 47-51). After processing by 14 or 12 acceptable packets are sent to buffer 28 and from there to network 30 (see col. 2 line 67 col. 3 line1 & col. 3 line 8-10); however buffer 28 in Applicant's view is not a second router and even if so construed there is nothing in the communication of these packets that has anything to do with routing or transmission or interrupting transmission of later or future packets.

Apparently the Examiner is construing one of the buffers or analysis stages or rules bases as the second router. Applicant submits that these can not be viewed as the second router required by the claim language. For example, if the Examiner is viewing the second buffer as the second router, there is no indication that forwarding a given low confidence packet or other packet to the second buffer will result in the second buffer interrupting a future data packet. As another example, Joyce speaks to shunting out of the Firewall to a log or supervisor. Presumably, this may result in some future improvements in transmission of troublesome packets, however these are not routers and these will not interrupt future packets. Similar reasoning may be applied to all other candidates for a second router or communicating therewith or communicating therewith pursuant to interrupting future transmissions in Applicant's respectfully considered view.

Therefore and at least in view of these reasons, Applicant submits that Joyce does not show or suggest all features of claim 1 or claim 11 or at least by virtue of dependency claims 2-10 and 12-20. Hence Joyce clearly does not anticipate claim 1 or claim 11 or at least by virtue of dependency claims 2-10 and 12-20. Applicant thus respectfully requests that the Examiner reconsider and withdraw the rejection of claims 1-20 under 35 U.S.C. 102(e) as being clearly anticipated by Joyce (US Patent No. 6,519,703).

Furthermore, one or more of the dependent claims recite additional features which are not shown or suggested by Joyce.

For example, claim 3 (and corresponding claim 13) recites sending a command to an upstream router to intercept future data packets from the originator. The Examiner maintains that "Joyce discloses sending a command to an upstream router (second buffer or control of disposition) to intercept future packets from the originator (Column 3 lines 5 - 54). As noted above, it is not appropriate to construe the second buffer as the required second router and furthermore even if so construed the second buffer is clearly downstream (in the direction of flow for the packet) rather than upstream (opposite to direction of flow) from the router (given that the first buffer is somehow viewed as the first router). Additionally there is nothing about any routing control at the second buffer that has anything to do with present commands effecting future packets.

Furthermore, claim 4 (and corresponding claim 14) recite forwarding an agent to an

upstream router, the agent arranged to intercept future data packets from the originator. The Examiner maintains that "Joyce discloses forwarding an agent to an upstream router, the agent arranged to intercept future data packets from the originator by forwarding control of disposition of packets and control logic (agent) is provided for intercepting data packets (Column 3 line 5 - Column 4 line 21). As noted above with reference to claim 3 there is no upstream communication suggested by Joyce and thus no possible upstream router and thus no agent is forwarded to an upstream router.

Additionally claim 7 (and corresponding claim 17) recites a feature where once a data packet has been deemed suspicious it is decided to monitor future data packets having the same source or destination address as claimed. The Examiner maintains that "Joyce discloses analyzing raw data packets originating from network with destination information also enter and the data that have high confidence are forwarded without analysis but the data that have poor-confidence (suspicious) and further analyzed for session traffic based on a combination of source and destination address (Column 4 line 14 - 60)."

Regarding a source or destination address, referred to by the Examiner state ",heuristic stage 48 operates upon ... session *data that has been translated into the frequency spectrum*, ... For example, data packet 22 flow can be represented as curves based on a combination of packet header information, such as source and destination addresses, ports, and time-stamp information. ... This information is analyzed for anomalies, discontinuities, and patterns that may indicate untrustworthy packets. Transforming time stamps into the frequency domain, for example, provides an opportunity to detect anomalies that are not detected by a time-domain analysis." Arguably these lines teach 'the use of source and destination addresses', but only when used in

conjunction with temporal analysis in the frequency domain. There is no indication, however, that any *predetermined* combination of source and destination address is being used. Joyce's curves are based on the consideration of packets from all source addresses and destination addresses. Curves are simply represented for each combination of addresses.

As a last example, Claims 8-10 (and corresponding claims 18-20) recite further features having to do with collaborating with and identifying an upstream router. None of these more specific features concerning an upstream router are shown or suggested by Joyce. The Examiner maintains that "Joyce discloses collaborating with and identifying an upstream router wherein a correlation analysis router operates on multi-directional session data that is based on source and destination address to call on external/alternate process (from participating routers like pager system or alerting systems) (Column 4 line 22 - Column 5 line 33).

Applicant notes once more that Joyce does not discuss or contemplate communication with an upstream router and thus these claims are not shown or suggested. The specific language cited by the Examiner refers to on technique for dealing with an anomaly that Joyce discusses at col. 4 line 64-67 and deals with an alternate process or flow control (see last paragraph col. 4).

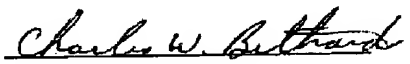
Therefore and at least for these additional reasons, Applicant respectfully submits that claims 3, 4, 7-10 and 13, 14, 17-20 are allowable over Joyce, since this reference does not show or suggest all features of any of these claims. Thus and in view of these additional reasons, Applicant respectfully requests that the Examiner reconsider and withdraw this rejection of claims 3, 4, 7-10 and 13, 14, 17-20 under 35 U.S.C. 102(e) based on Joyce (U.S. Patent No. 6,519,703).

Accordingly, Applicant respectfully submits that the claims clearly and patentably distinguish over the cited reference of record and as such are to be deemed allowable. Such allowance is hereby earnestly and respectfully solicited at an early date. If the Examiner has any suggestions or comments or questions, calls are welcomed at the phone number below.

This response is being filed within two months of the mailing date of a Final Office Action and thus Applicant anticipates that the period for response will not lapse until the later of the original three month period or the date of mailing any communication resulting from a consideration of these comments.

Although it is not anticipated that any fees are due or payable, the Commissioner is hereby authorized to charge any fees that may be required to Deposit Account No. **50-3435**.

Respectfully submitted,



Charles W. Bethards
Reg. No. 36,453

Law Office of Charles W. Bethards, LLP
P.O. Box 1622
Colleyville, Texas 76034
Phone (817) 581-7005
Fax (817) 281-7136
Customer No. 51874